AMENDMENTS TO THE CLAIMS

1. (Previously presented) An integrated circuit implementing at least one operator involving at least one secret quantity, and functionally comprising upstream and downstream of the operator at least first and second source registers and at least one destination register, respectively, at least one temporary register means for loading a first random or pseudo-random number into the temporary register, means for transferring the content of the first source register to the temporary register, and means for loading a second random or pseudo-random number into the destination register, the operator combining the content of the second source register and the temporary register and storing the result in the destination register.

2. - 3. (Canceled)

4. (Previously presented) An antifraud method comprising randomizing a content of a destination register of a result of an operator involving at least one secret quantity, and inputting a random quantity in the destination register before each loading of a result therein, further comprising loading a first random or pseudo-random number into a temporary register, transferring the content of a first source register to the temporary register, loading a second random or pseudo-random number into the destination register, the operator combining the content of a second source register and the temporary register and storing the result in the destination register.

5. (Canceled)

6. (Previously presented) An integrated circuit comprising:
an operator configured to perform an operation on a secret quantity;
a destination register coupled to receive a result of the operation;
first and second source registers;
a temporary register; and

a control circuit configured to load a first random or pseudo-random number into the temporary register, to transfer the content of the first source register to the temporary register, and to load a second random or pseudo-random number into the destination register, the operator combining the content of the second source register and the temporary source register and storing the result in the destination register.

7.-10. (Canceled)

11. (Original) An integrated circuit as defined in claim 6, wherein the destination register is a source register for a second operator.

12. (Previously presented) An antifraud method comprising:

randomizing a content of a destination register coupled to receive a result of an operation involving a secret quantity before transfer of a result into the destination register, to protect against attacks by physical signature analysis, further comprising loading a first random or pseudo-random number into a temporary register, transferring the content of a first source register to the temporary register, loading a second random or pseudo-random number into the destination register, the operator combining the content of a second source register and the temporary register and storing the result in the destination register.

13.-16. (Canceled)

17. (Original) An antifraud method as defined in claim 12, further comprising using the destination register as a source register for a second operation.

18. (Previously presented) An antifraud method comprising:

loading a first random or pseudo-random number into a temporary register;

transferring the content of a first source register to the temporary register;

performing an operation on a secret quantity to produce a result, the operation combining the content of a second source register and the temporary register;

loading a random or pseudo-random number into a destination register that is coupled to receive the result of the operation, to protect against attacks by physical signature analysis; and

transferring the result of the operation into the destination register.

19.-20. (Canceled)